PCT

WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 6 :
G07F 7/10, G07C 9/00

A1

(11) International Publication Number: WO 00/28493

(43) International Publication Date: 18 May 2000 (18.05.00)

(21) International Application Number: PCT/SG98/00088

(22) International Filing Date: 10 November 1998 (10.11.98)

(71) Applicant *(for all designated States except US)*: KENT RIDGE DIGITAL LABS [SG/SG]; 21 Heng Mui Keng Terrace, Singapore 119613 (SG).

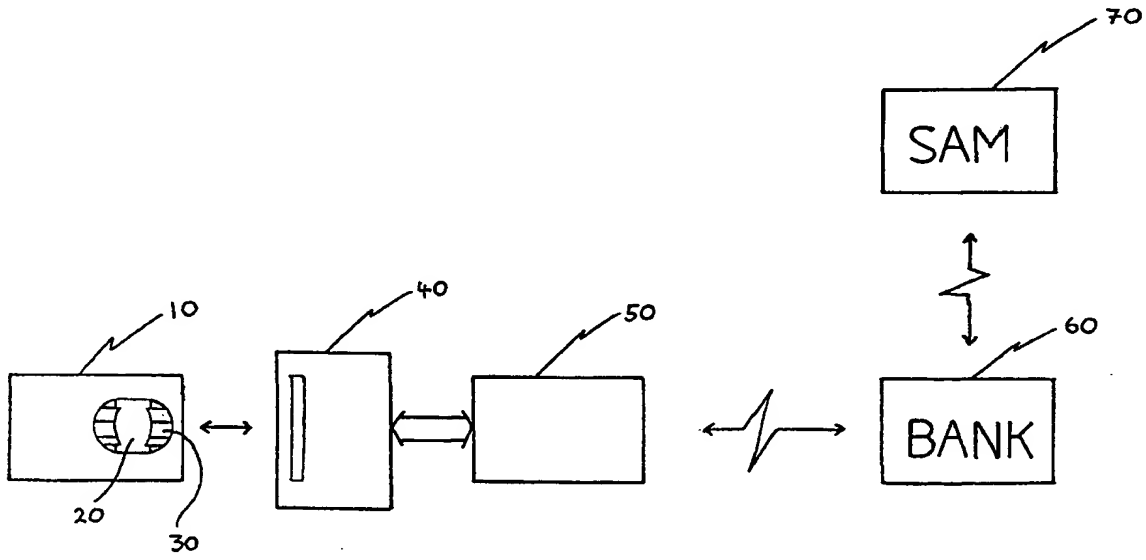
(72) Inventor; and
(75) Inventor/Applicant *(for US only)*: NGAIR, Teow, Hin [SG/SG]; 334 Kang Ching Road #13–254, Singapore 610334 (SG).

(74) Agent: GREENE–KELLY, James, Patrick; Lloyd Wise, Tanjong Pagar, P.O. Box 363, Singapore 910816 (SG).

(81) Designated States: AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CU, CZ, DE, DK, EE, ES, FI, GB, GE, GH, GM, HR, HU, ID, IL, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, UA, UG, US, UZ, VN, YU, ZW, ARIPO patent (GH, GM, KE, LS, MW, SD, SZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

Published
With international search report.

(54) Title: A METHOD OF ENCRYPTION AND APPARATUS THEREFOR



(57) Abstract

A method of encryption for creating token bound output data from user data using a symmetric key capable token is disclosed, said method comprising the steps of providing the user data or a representation thereof as an input to a symmetric key operation supported by the token, retrieving the output of the symmetric key operation as the token signature; and combining the token signature with the user data to generate the token bound output data. Preferably the output data is used as an input parameter to a private key signature generation operation, to form a private key signature for the user data.

FOR THE PURPOSES OF INFORMATION ONLY

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AL	Albania	**ES**	Spain	**LS**	Lesotho	**SI**	Slovenia
AM	Armenia	**FI**	Finland	**LT**	Lithuania	**SK**	Slovakia
AT	Austria	**FR**	France	**LU**	Luxembourg	**SN**	Senegal
AU	Australia	**GA**	Gabon	**LV**	Latvia	**SZ**	Swaziland
AZ	Azerbaijan	**GB**	United Kingdom	**MC**	Monaco	**TD**	Chad
BA	Bosnia and Herzegovina	**GE**	Georgia	**MD**	Republic of Moldova	**TG**	Togo
BB	Barbados	**GH**	Ghana	**MG**	Madagascar	**TJ**	Tajikistan
BE	Belgium	**GN**	Guinea	**MK**	The former Yugoslav Republic of Macedonia	**TM**	Turkmenistan
BF	Burkina Faso	**GR**	Greece			**TR**	Turkey
BG	Bulgaria	**HU**	Hungary	**ML**	Mali	**TT**	Trinidad and Tobago
BJ	Benin	**IE**	Ireland	**MN**	Mongolia	**UA**	Ukraine
BR	Brazil	**IL**	Israel	**MR**	Mauritania	**UG**	Uganda
BY	Belarus	**IS**	Iceland	**MW**	Malawi	**US**	United States of America
CA	Canada	**IT**	Italy	**MX**	Mexico	**UZ**	Uzbekistan
CF	Central African Republic	**JP**	Japan	**NE**	Niger	**VN**	Viet Nam
CG	Congo	**KE**	Kenya	**NL**	Netherlands	**YU**	Yugoslavia
CH	Switzerland	**KG**	Kyrgyzstan	**NO**	Norway	**ZW**	Zimbabwe
CI	Côte d'Ivoire	**KP**	Democratic People's Republic of Korea	**NZ**	New Zealand		
CM	Cameroon			**PL**	Poland		
CN	China	**KR**	Republic of Korea	**PT**	Portugal		
CU	Cuba	**KZ**	Kazakstan	**RO**	Romania		
CZ	Czech Republic	**LC**	Saint Lucia	**RU**	Russian Federation		
DE	Germany	**LI**	Liechtenstein	**SD**	Sudan		
DK	Denmark	**LK**	Sri Lanka	**SE**	Sweden		
EE	Estonia	**LR**	Liberia	**SG**	Singapore		

INTERNATIONAL SEARCH REPORT

International application No.
PCT/SG 98/00088

A. CLASSIFICATION OF SUBJECT MATTER

IPC[6]: G 07 F 7/10; G 07 C 9/00

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

IPC[6]: G 06 F; G 07 F; G 07 C

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

EPODOC

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	EP 0 837 383 A2 (FUJI XEROX) 22 April 1998 (22.04.98), claims 1,2,21; fig.1,2.	1,12
A	US 5 280 527 A (KAMAHIRA SAFE) 18 January 1994 (18.01.94), claims 1,6; fig.1-3.	1,2,12,16
A	WO 98/22 914 A1 (TECSEC INC.) 28 May 1998 (28.05.98), claims 1,5,14-20; fig..	1,12
A	EP 0 735 720 A1 (PITNEY BOWES) 02 October 1996 (02.10.96), claims 1,5; fig.1.	1,12
A	EP 0 624 014 A1 (FISCHER) 09 November 1994 (09.11.94), claims 1,4,7; fig.1.	1,12,16
A	US 3 806 704 A (SHINAI) 23 April 1974 (23.04.74).	1,12,16

☐ Further documents are listed in the continuation of Box C. ☒ See patent family annex.

* Special categories of cited documents:
„A" document defining the general state of the art which is not considered to be of particular relevance
„E" earlier application or patent but published on or after the international filing date
„L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
„O" document referring to an oral disclosure, use, exhibition or other means
„P" document published prior to the international filing date but later than the priority date claimed
„T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
„X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
„Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
„&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
07 June 1999 (07.06.99)	29 June 1999 (29.06.99)
Name and mailing adress of the ISA/AT Austrian Patent Office Kohlmarkt 8-10; A-1014 Vienna Facsimile No. 1/53424/200	Authorized officer Mihatsek Telephone No. 1/53424/329

Form PCT/ISA/210 (second sheet) (July 1998)

(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

CORRECTED VERSION

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
18 May 2000 (18.05.2000)

PCT

(10) International Publication Number
WO 00/28493 A1

(51) International Patent Classification[6]: G07F 7/10, G07C 9/00

(21) International Application Number: PCT/SG98/00088

(22) International Filing Date:
10 November 1998 (10.11.1998)

(25) Filing Language: English

(26) Publication Language: English

(71) Applicant *(for all designated States except US)*: **KENT RIDGE DIGITAL LABS** [SG/SG]; 21 Heng Mui Keng Terrace, Singapore 119613 (SG).

(72) Inventor; and

(75) Inventor/Applicant *(for US only)*: **NGAIR, Teow, Hin** [SG/SG]; 334 Kang Ching Road #13-254, Singapore 610334 (SG).

(74) Agent: **GREENE-KELLY, James, Patrick**; Lloyd Wise, Tanjong Pagar, P.O. Box 636, Singapore 910816 (SG).

(81) Designated States *(national)*: AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CU, CZ, DE, DK, EE, ES, FI, GB, GE, GH, GM, HR, HU, ID, IL, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, UA, UG, US, UZ, VN, YU, ZW.

(84) Designated States *(regional)*: ARIPO patent (GH, GM, KE, LS, MW, SD, SZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

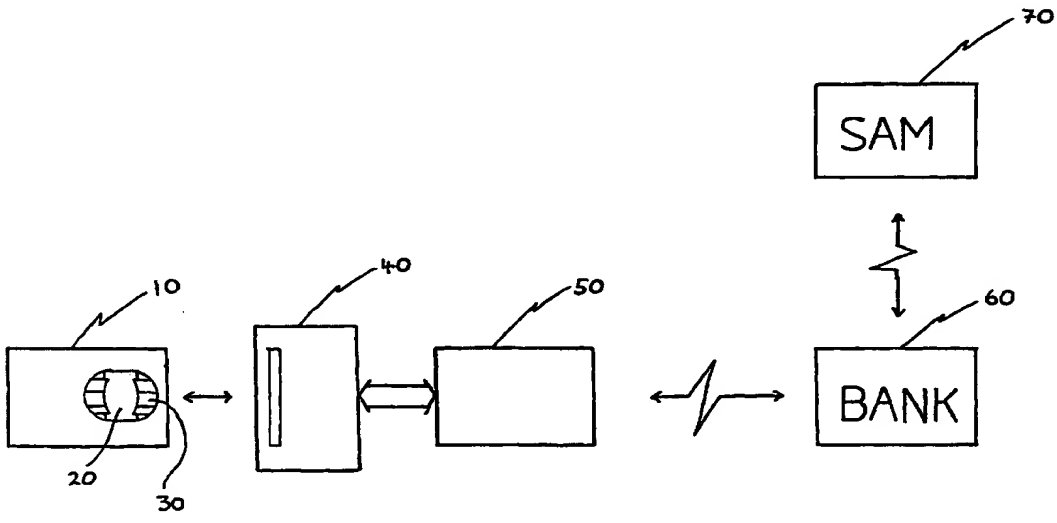
Published:
— *With international search report.*

(48) Date of publication of this corrected version:
1 February 2001

(15) Information about Correction:
see PCT Gazette No. 05/2001 of 1 February 2001, Section II

[Continued on next page]

(54) Title: A METHOD OF ENCRYPTION AND APPARATUS THEREFOR



(57) Abstract: A method of encryption for creating token bound output data from user data using a symmetric key capable token is disclosed, said method comprising the steps of providing the user data or a representation thereof as an input to a symmetric key operation supported by the token, retrieving the output of the symmetric key operation as the token signature; and combining the token signature with the user data to generate the token bound output data. Preferably the output data is used as an input parameter to a private key signature generation operation, to form a private key signature for the user data.

WO 00/28493 A1

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/SG 98/00088

In Recherchenbericht angeführtes Patentdokument Patent document cited in search report Document de brevet cité dans le rapport de recherche	Datum der Veröffentlichung Publication date Date de publication	Mitglied(er) der Patentfamilie Patent family member(s) Membre(s) de la famille de brevets	Datum der Veröffentlichung Publication date Date de publication
EP A2 837383	22-04-1998	JP A2 10123950	15-05-1998
US A 5280527	18-01-1994	CA AA 2105404	03-03-1995
WO A 9822914		keine - none - rien	
EP 735720		BR A 9601232	06-01-1998
		CA AA 2172860	01-10-1996
		CN A 1144942	12-03-1997
		EP A2 735720	02-10-1996
		JP A2 9167186	24-06-1997
		US A 5661803	26-08-1997
EP 624014		AU A1 57781/94	17-11-1994
		AU B2 666424	08-02-1996
		CA AA 2120665	06-11-1994
		CA C 2120665	22-12-1998
		EP A2 624014	09-11-1994
		EP A3 624014	08-03-1995
		EP A2 770953	02-05-1997
		EP A3 770953	15-10-1997
		EP A2 841604	13-05-1998
		JP A2 7254897	03-10-1995
		US A 5422953	06-06-1995
US A 3806704	23-04-1974	keine - none - rien	

EO/US
PCT/SG98/00088

PATENT COOPERATION TREATY

From the INTERNATIONAL BUREAU

PCT

NOTIFICATION OF ELECTION

(PCT Rule 61.2)

To:

Assistant Commissioner for Patents
United States Patent and Trademark Office
Box PCT
Washington, D.C.20231
ETATS-UNIS D'AMERIQUE

in its capacity as elected Office

Date of mailing: 18 May 2000 (18.05.00)	
International application No.: PCT/SG98/00088	Applicant's or agent's file reference: FP1110
International filing date: 10 November 1998 (10.11.98)	Priority date:
Applicant: NGAIR, Teow, Hin	

1. The designated Office is hereby notified of its election made

[X] in the demand filed with the International preliminary Examining Authority on:

27 March 2000 (27.03.00)

[ ] in a notice effecting later election filed with the International Bureau on:

2. The election [X] was

[ ] was not

made before the expiration of 19 months from the priority date or, where Rule 32 applies, within the time limit under Rule 32.2(b).

The International Bureau of WIPO
34, chemin des Colombettes
1211 Geneva 20, Switzerland

Facsimile No.: (41-22) 740.14.35

Authorized officer:

J. Zahra

Telephone No.: (41-22) 338.83.38

Copy for the elected Office (EO/US)

PATENT COOPERATION TREATY

From the INTERNATIONAL BUREAU 09831491

PCT

COMMUNICATION IN CASES FOR WHICH NO OTHER FORM IS APPLICABLE

To:
GREENE-KELLY, James, Patrick
Lloyd Wise
Tanjong Pagar
P.O. Box 636
Singapore 910816
SINGAPOUR

Date of mailing (*day month year*) 29 November 2002 (29.11.02)	
Applicant's or agent's file reference FP1110	**REPLY DUE** **see paragraph 1 below**
International application No. PCT/SG98/00088	International filing date (*day/month/year*) 10 November 1998 (10.11.98)
Applicant KENT RIDGE DIGITAL LABS	

1. ☐ REPLY DUE within _____ months/days from the above date of mailing

☐ NO REPLY DUE, however, see below

☐ IMPORTANT COMMUNICATION

☒ INFORMATION ONLY

2. COMMUNICATION:

The International Bureau regrets to inform the applicant that due to a clerical error above mentioned international application has been withdrawn on 02 September 2002 (02.09.02).

It is herewith confirmed that the application has been reinstated and that the notification PCT/IB/325 "Notification that international application considered to be withdrawn", issued on the same date should be considered null and void.

A copy of this communication has been sent to the receiving Office and all designated Offices concerned.

The International Bureau of WIPO 34, chemin des Colombettes 1211 Geneva 20, Switzerland	Authorized officer Peggy Steunenberg